bearing insurance®

Preparing for National Cybersecurity Awareness Month

October 2025 marks the 22nd annual Cyber Awareness Month, during which government and industry leaders come together to raise awareness about the importance of cybersecurity and cyber insurance. This month serves as a reminder that businesses must stay cybersecure to safeguard company data, protect customers' personal information, and ensure employee privacy.

Here are four strategies from the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance that businesses and their employees can use to stay cybersecure throughout the year:

- **Use strong passwords and password managers.** Cybercriminals are often able to determine or guess simple passwords. Businesses should require employees to use strong passwords for all work-related accounts. Passwords should be at least 16 characters long, random, and unique for each account. The use of password managers — secure programs that maintain and create passwords — should be encouraged or required. These easy-to-use programs store passwords and fill them in automatically on the web.

- **Implement multifactor authentication (MFA).** MFA is a layered approach to securing data and applications. This tool requires a user to present a combination of two or more credentials to verify their identity for login. MFA enhances security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database. Businesses should enable MFA on any site or service that offers it.

- **Recognize and report phishing.** Many cyberattacks result from a recipient of a phishing message accidentally downloading malware or giving sensitive information to a cybercriminal. Therefore, employees should know the signs of a phishing attack and be instructed not to click on or engage with these phishing attempts. Instead, employees should recognize them by their use of alarming language or offers that are too good to be true. Phishing attempts should be reported using the appropriate IT protocols. If a business suspects that it has become a victim of a phishing attack (or any other type of cybercrime), it should immediately report the incident to its insurance partners and the appropriate government authorities.

- **Update software.** Businesses should ensure their software programs stay up to date by installing security updates as soon as possible. These updates close security vulnerabilities and help protect organizations from cyberattacks.

For more information on Cybersecurity Awareness Month, review CISA's webpage for the observance. Contact us today for more cybersecurity guidance and cyber insurance solutions.

bearing insurance®

Personal Cyber Coverage and Commercial Cyber Liability Insurance Explained

Personal Cyber Coverage

As society becomes more digital, smart devices are increasingly part of daily life. While this technology offers many benefits, it also raises the risk of cybercrime. With cyber threats on the rise, protecting yourself and your family is essential. Personal cyber insurance — typically added to a homeowners policy — can help cover losses from incidents like fraud, identity theft, and data breaches. Key coverages often include online fraud, identity recovery, cyberbullying, and more.

Here are some of the most common cyber incident scenarios that individuals and their families may encounter:

- **Bank fraud.** This form of fraud entails a cybercriminal gaining unauthorized access to an individual's electronic bank credentials, allowing them to transfer and steal funds from the individual's account. According to a recent report from NortonLifeLock, cybercriminals steal over $170 billion each year via bank fraud.
- **Identity theft.** This type of theft refers to a cybercriminal accessing an individual's personal information and using it to commit fraud or other crimes under the individual's name. The Federal Trade Commission confirmed that nearly 1.4 million complaints related to identity theft were filed last year, up 113% from the previous year.
- **Data loss.** In the event that an individual's device gets infected with a virus or other malicious software, they face the risk of losing any valuable data stored on that device. Viruses and malware can come from numerous avenues, thus making data loss a major threat.
- **Extortion.** Ransomware incidents have contributed to a substantial rise in cyber extortion over the last few years. These incidents stem from a cybercriminal using malware to compromise an individual's device (and any data stored on it) and demanding a ransom payment in exchange for restoration. According to cybersecurity experts, ransomware incidents have increased 500% since 2018, with the average ransom payment totaling over $300,000.
- **Cyberbullying.** While social media platforms allow individuals to connect with others, these platforms can also, unfortunately, be used for negative purposes, such as cyberbullying. The latest data from Pew Research revealed that 59% of teens have experienced cyberbullying.

Considering these risks, it's clear that individuals can't afford to ignore cybercrime. In addition to implementing effective cybersecurity practices, having adequate insurance in place is crucial. By investing in personal cyber coverage, individuals can properly protect themselves and their families amid cyber-related losses.

bearing insurance®

Cyber Liability Insurance

As technology becomes increasingly important for successful business operations, the value of a strong cyber liability insurance policy will only continue to grow. The ongoing rise in the amount of information stored and transferred electronically has resulted in a significant increase in the potential exposures facing businesses. In an age where a stolen laptop or hacked account can instantly compromise the personal data of thousands of customers — or an ill-advised post on social media can be read by hundreds within minutes — protecting yourself from cyber liability is just as important as the more traditional exposures businesses account for in their general commercial liability policies.

Possible exposures covered by a typical cyber liability policy may include the following:

- **Data breaches.** Stricter regulations now require companies to protect client data and notify affected parties in the event of a breach — adding costs for security fixes, identity protection, and potential legal action. Even businesses that don't transmit data online but store it electronically are at risk from unauthorized access or hardware theft.
- **Intellectual property rights.** Your company's online presence opens you up to some of the same exposures faced by publishers. This can include libel, copyright or trademark infringement, and defamation, among other risks.
- **Damages to a third-party system.** If an email sent from your server contains a virus that crashes a customer's system, or if software your company distributes fails and causes a loss for a third party, you could be held liable for the damages.
- **System failure.** A natural disaster, malicious activity, or fire could cause physical damage resulting in data or code loss. While physical damage to your system hardware may be covered under your existing business liability policy, data or code loss due to the incident would not be.
- **Cyber extortion.** Hackers can hijack websites, networks, and stored data, denying access to you or your customers. This can lead to temporary revenue loss and costs associated with paying the hacker's demands or rebuilding damaged systems.
- **Business interruption.** If your operations rely on computer systems, a disruption — like server failure or a data breach — can halt productivity and lead to revenue loss. Resources may need to be redirected to resolve the issue, causing further delays. Denial-of-service attacks, which block access by overloading servers or rerouting traffic, are becoming increasingly common.

Cyber liability insurance is specifically designed to address the risks that come with using modern technology. The level of coverage your business needs depends on your individual operations and can vary based on your range of exposure. It's important to work with a broker who can identify your areas of risk and tailor a policy to fit your unique situation.

As reliance on technology grows, so do the risks for individuals and businesses alike. Whether you're protecting personal data at home or securing sensitive information across your organization, cyber insurance is essential. Bearing Insurance is here to help safeguard you throughout your insurance journey. Contact us today to learn how our expertise and commitment can help protect your future.